REMARKS

Claims 1-13 and 15-25 are pending in the present application. Claims 1 and 13 are independent.

35 U.S.C. § 103(a) Rejections

Claims 1-13 and 15-25 have been rejected under 35 U.S.C. § 103(a) over Ishiguro (European Patent Application EP 0856821) in view of Barlow (US Patent Publication No 2004/0215964) and further in view of Deindl (US Patent No. 6,076,162). Applicants respectfully traverse the rejection. Claims 1-13 and 15-25 include features that are neither disclosed nor suggested by the art of record as represented by claim 1 which recites:

> 1. A method for checking a digital signature, involving a microcircuit connectable to a data processing system, the microcircuit being designed to receive requests to check digital signatures from the data processing system, and to process these requests, a digital signature being generated using a private key only known to a signatory entity and associated with a public key, said method comprising a step of ***storing a certificates table containing a digest form of at least one public key*** in a memory in the microcircuit, and a phase of checking a digital signature comprising steps of:
>
> receiving by the microcircuit a digital signature to be checked and a public key in a pair of keys comprising a private key that was used to generate the digital signature to be checked,
>
> calculating a digest form of the received public key, and
>
> ***searching for the calculated digest form of the public key in the certificates table***, and
>
> decrypting the digital signature using the received public key if the calculated digest form of the public key is located in the certificates table. (emphasis added)

Claim 1 recites storing a digest form of a public key. Claim 1 further recites searching for the digest form of the public key in a certificates table. If a match is found (e.g., the digest

form of the public key is in the certificates table), then the digital signature is decrypted. By storing and searching the digest form of the public key, memory could be saved. None of the cited references disclose or suggest storing and searching for a digest form of a public key, as recited by the claims.

The examiner relies only on Deindl for the digest form of a public key and thus, only Deindl is discussed in detail herein. Deindl describes a procedure for the certification of cryptographic keys for use in chipcards. The procedure includes the following steps:

- transferring to the chipcard a certificate composed of a first part including administrative information and the public key (see Deindl at Table l), and a second part including a digital signature of the first part, ***the first part being stored on the chipcard*** (Deindl at col. 2 lines 42-52, col. 5 lines 52-53, and col. 3 lines 46-51);

- checking that the second part corresponds to the digital signature of the first part by using a ***certification key stored in the chipcard*** (Deindl at col. 2 lines 42-47, col. 5 line 61 - col. 6 line 21); and

- if this is the case, marking the public key contained in the first part of the certificate and stored on the chipcard as certified (Deindl at col. 6 lines 19-20, lines 39-58).

Deindl stores certified cryptographic keys in the chipcard (see in particular col. 2 lines 45-55, "It can be made certain in this way that only those keys which have been correctly transferred to the chipcards and correctly stored in the chipcards can be used as certified keys", and col. 3 lines 46-52, "'it can be provided that the marking of the cryptographic key as a certified key can be carried out by entering the cryptographic key in a table on the chipcard. In this way, all certified keys can be stored in the chipcard in a manner which can be inspected".). In contrast, claim 1 recites storing the digest form of a public key.

Further, when Deindl searches, it searches for the full certified cryptographic key rather than searching for the digest form of the public key in the certificates table, as recited by claim 1.

By storing the certified cryptographic keys on the chipcard and searching for certified cryptographic keys, Deindl may require a larger memory capacity on the chipcard. This deficiency has been noted in the instant patent application, as-filed, at page 3 lines 8-15.

Therefore, none of Ishiguro, Barlow, and Deindl disclose or suggest a ***storing a certificates table containing a digest form of at least one public key*** or ***searching for the calculated digest form of the public key in the certificates table***, as recited by claim 1.

Claim 13 contains features that are similar to those of claim 1, and is therefore allowable for at least the reasons stated in connection with claim 1. Claims 2-12, and 15-25 are dependent on claims 1 or 13, and are therefore allowable for at least the reasons given for claims 1 and 13. Applicants respectfully request that the Examiner withdraw the rejection and allow claims 2-13 and 15-25.

Conclusion

It is believed that all of the pending issues have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this reply should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this reply, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment. Applicants submit that all claims are in condition for allowance.

Please apply any required charges or any credits to deposit account 06-1050 referencing the above Attorney Docket No. 18394-0009US1.

Respectfully submitted,

Date: March 24, 2009

Raymond N. Scott, Jr.
Reg. No. 48,666

Fish & Richardson P.C.
P.O. Box 1022
Minneapolis, MN 66550-1022
Telephone: (302) 652-5070
Facsimile: (877) 769-7945

80076603.doc